



The 2014 Home Depot Data Breach: A Cybersecurity Case Study

Andrew Burbage

Computer Science, Charleston Southern University

CSCI 405

Dr. Sun

02-25-2026

Introduction & Overview

- The largest retail card breach at the time (2014).
 - Impact:
 - ~56 million payment cards compromised.
 - ~53 million customer email addresses stolen.
 - Timeline: April 2014 – September 2014.
-

The Attack Timeline

Nov 2013

Entry

Initial network entry via stolen third-party vendor credentials.

Apr 2014

Deployment

Hackers deploy malware to self-checkout systems.

Sept 2, 2014

Alert and Investigation

Investigation begins after banking partner alerts.

Sept 18, 2014

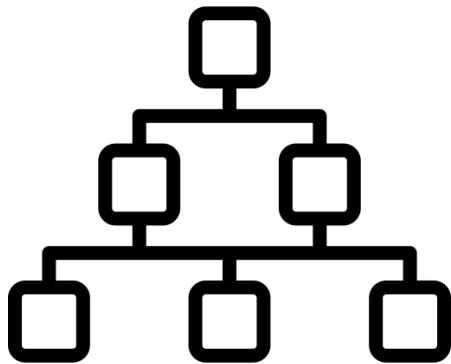
Official Confirmation

Home Depot officially confirms breach details.



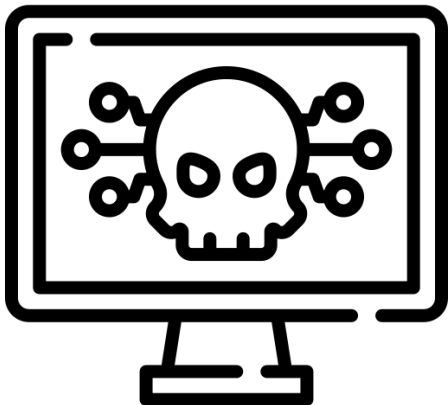
Technical Breakdown: Initial Access

- **Attack Vector:** Stolen credentials from a third-party vendor.
- **Method:** Hackers used these credentials to enter the perimeter of the corporate network.
- **Failure:** Lack of Multi-Factor Authentication (MFA) on vendor access points.



Technical Breakdown: Lateral Movement

- Exploitation of unpatched Windows vulnerabilities.
- Elevation of privileges to gain administrative rights.
- Navigation from corporate network to the payment card environment.



The Malware: "RAM Scraper"

- **Name:** Variant of "BlackPOS" (Kaptoxa).
- **Function:** Designed to scrape data from the RAM of POS terminals.
- **Unique Feature:** "Custom-built" to evade standard antivirus detection.

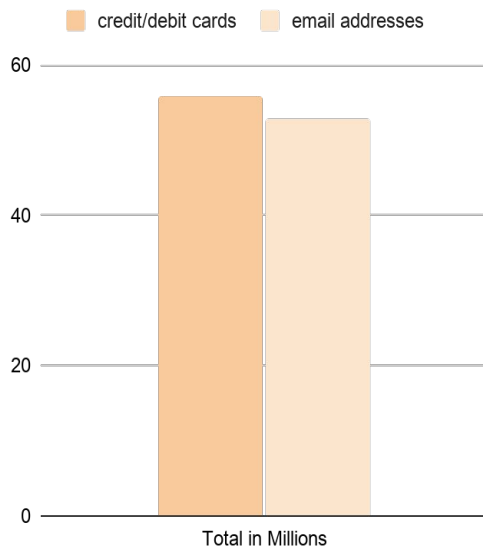


Data Exfiltration

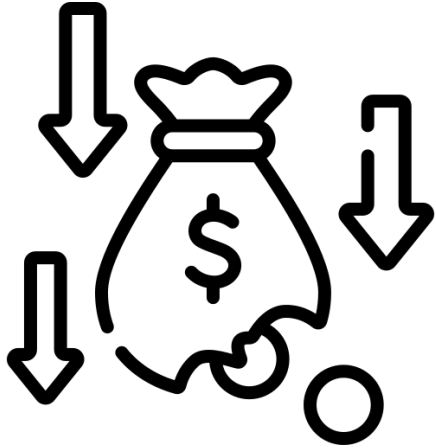
- Targeted the magnetic strip data (Track 2 data).
- Data Included: Name, Card Number, Expiration, CVV.
- Data was bundled and sent to offsite attacker-controlled servers.

Impact on Consumers

P.I.I. Exposure



- 56 million unique credit/debit cards exposed.
 - 53 million email addresses (separate files).
 - **Risk:** Identity theft, fraudulent charges, and phishing.
-



Financial Impact

- Total estimated cost: Over \$179 million.
- Settlement with consumers: \$19.5 million.
- Settlement with financial institutions: ~\$27 million.
- Legal and remediation costs: Over \$150 million.

Legal & Regulatory Fallout

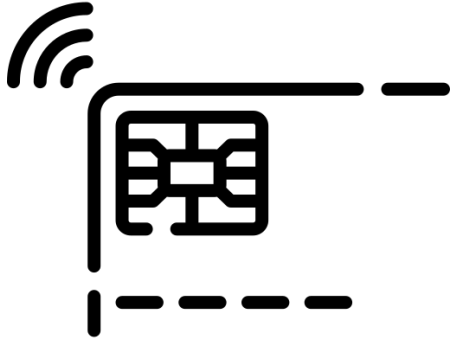


- 2020 Multi-state Settlement: \$17.5 million (46 states + D.C.).
- Mandated security reforms.
- Appointment of a Chief Information Security Officer (CISO).



Remediation: Immediate Actions

- Malware elimination from all U.S. and Canadian networks.
- Enhanced encryption (Voltage Security) rolled out to all U.S. stores by Sept 13, 2014.
- Free identity protection/credit monitoring for customers.



Remediation: Long-term Security

- EMV "Chip and PIN" technology rollout.
- Network segmentation (isolating POS systems).
- Strict third-party vendor management and MFA.

Cybersecurity Lessons Learned



- **Vendor Risk:** Third parties are the "weakest link."
- **Patch Management:** Critical vulnerabilities must be patched immediately.
- **Detection Gap:** Five months is too long; improved logging and monitoring are vital.

Conclusion

- Home Depot 2014 serves as a blueprint for retail vulnerabilities.
 - Transitioned from reactive to proactive security.
 - Demonstrates the high cost of "security debt" (unpatched systems).
-

References

- Berkeley Technology Law Journal (BTLJ). (2015). *Here comes another one: Examining the Home Depot data breach lawsuit*. <https://btlj.org/2015/01/here-comes-another-one-examining-the-home-depot-data-breach-lawsuit/>
 - Flaticon. (2024). *Cybersecurity and technology icon set* [Icons]. <https://www.flaticon.com>
 - Home Depot. (2014a, September 18). *The Home Depot provides update on breach investigation*. <https://ir.homedepot.com/news-releases/2014/09-18-2014-014517752>
 - Home Depot. (2014b, November 6). *The Home Depot reports findings in payment data breach investigation*. <https://ir.homedepot.com/news-releases/2014/11-06-2014-014517315>
 - The Home Depot. (n.d.). *The Home Depot logo* [Logo]. <https://corporate.homedepot.com/media/home-depot-logoipg>
 - Office of the Attorney General of New York. (2020, November 24). *Attorney General James helps secure \$17.5 million after data breach at The Home Depot*. <https://ag.ny.gov/press-release/2020/attorney-general-james-helps-secure-175-million-after-data-breach-home-depot>
-

References (Continued)

- Reuters. (2020, November 24). *Home Depot reaches \$17.5 mln settlement over 2014 data breach.*
<https://www.reuters.com/business/home-depot-reaches-175-mln-settlement-over-2014-data-breach-2020-11-24/>
 - SANS Institute. (2015). *Case study: The Home Depot data breach.*
<https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367>
 - Wall Street Journal. (2014, September 8). *Home Depot confirms data breach.*
<https://www.wsj.com/articles/home-depot-confirms-data-breach-1410209720>
-